ILLINOIS JOURNAL OF MATHEMATICS
Volume 26, Number 3, Fall 1982

A RECURSION FORMULA WITH APPLICATIONS TO ALGEBRA, NUMBER THEORY AND COMBINATORICS

BY

PETER WILKER

0. Introduction

In this paper we shall derive a recursion formula connecting counting functions of generalized graded monoids. (See Section 1 for details). The proof of this formula will be obtained by elementary arguments.

By specializing the monoids the recursion formula leads to a wide variety of formulae in algebra, number theory and combinatorics, most of them derived independently and usually by means of generating functions.

Section 1 states the precise meaning of "generalized graded monoid", while Section 2 gives a proof of the recursion formula. The remaining sections contain applications.

The author wishes to thank his friend and colleague, Professor Jany Binz, for valuable advice and many helpful discussions.

1. Generalized graded monoids

Throughout this paper, G and M will denote monoids: G will be called the grading, M the graded monoid.

G, written additively and with 0 as its identity, is required to be commutative and cancellative, as well as to possess the following properties: for every fixed $g \in G$, the set of solutions (u, v) of $g = u + v$ is finite; for $g = 0$ it is unique, viz. $(0, 0)$.

We define an order relation on G by setting $a \leq b$ if and only if the equation $a + x = b$ is solvable. The solution of this equation, if it exists, is unique by the cancellation law and shall be denoted by $b - a$.

Indeed, $\leq$ is an order relation. Reflexivity and transitivity are trivial. If $a \leq b$ and $b \leq a$, then, for some x and y, $a + x = b$, $b + y = a$ and $a + (x + y) = a$. Hence $x + y = 0$ and $x = y = 0$, whence $a = b$.

We list without proof the following properties of G:

$(G, \leq)$ is locally finite; i.e., for any $g \in G$ the set $\{h: h \leq g\}$ is finite.

For a natural number n, let $n \,.\, g$ denote the sum of n elements g. If $n \,.\, g = 0$, then $g = 0$.

$0 \leq g$ for all $g \in G$.

Received November 6, 1980.

PROPOSITION 1. *Let a, b be two non-zero elements of G with $a \leq b$. There is a uniquely determined natural number $q = q(a, b)$ such that $i \,.\, a \leq b$ if and only if $i \leq q$.*

Proof. The set $\{i\colon i \,.\, a \leq b\}$ is finite; let q be its maximal member. Then $i \,.\, a \leq b$ implies $i \leq q$. Suppose, on the other hand, that $j < q$; then

$$q \,.\, a = j \,.\, a + (q - j) \,.\, a \leq b$$

and there is an x such that $j \,.\, a + (q - j) \,.\, a + x = b$. This implies $j \,.\, a \leq b$.

M will be written multiplicatively, with 1 as its identity, and will be required to be commutative. The notions of unit, irreducible and associated elements shall have their usual meaning. There is an equivalence relation defined by the notion of associated elements. Its quotient structure on M is again a commutative monoid, but with 1 as its only unit. In the sequel, we shall only use this structure and shall call it again M.

Suppose a degree function deg: $M \to G$ has been defined with

$$\deg(m_1 m_2) = \deg m_1 + \deg m_2 \quad \text{for all } m_1, m_2 \in M.$$

Obviously, $\deg 1 = 0$. We postulate for $(G, M, \deg)$: for a given $g \in G$, there are only finitely many elements of M with degree g; if $g = 0$, there is only one, viz. 1.

PROPOSITION 2. *Every element of M is a product of irreducibles. While the representation need not be unique, there are only finitely many representations as products of irreducibles for any given element of M.*

Proof. If $m \in M$ is not irreducible, then $m = m_1 m_2$ for some $m_1, m_2 \in M$, both different from 1. As $\deg m = \deg m_1 + \deg m_2$, if $\deg m = \deg m_1$, then by the cancellation law for G we arrive at $\deg m_2 = 0$, which is impossible. Hence $\deg m_1, \deg m_2 < \deg m$. As there are only finitely many elements of G less then a given one, and because of our assumptions about M, we proved our claim.

For $m \in M$, let $R(m)$ denote the number of representations of m as a product of irreducibles. For $n \in G$, $P(n)$ will always denote $\sum R(m)$, where the sum is to be extended over all elements m of degree n. Of course, if the monoid M admits unique representation by irreducibles, $P(n)$ just counts the number of elements of degree n. The number of irreducible elements of degree n will be denoted by $I(n)$.

Let $d, k \in G$. If there is a natural number i such that $i \,.\, d = k$, we shall write $d \mid k$. Obviously, $i = q(d, k)$; we shall use the notation $q(d, k) = k/d$ in this case.

Let $\mathbf{N}$ denote the multiplicative monoid of natural numbers, $\mathbf{N}_0$ the additive monoid of non-negative integers.

2. The recursion formula

The main topic of this paper will be a proof and applications of the following:

THEOREM. *The notations of Section* 1 *taken for granted, the following recursion formula holds*:

$$\text{(RF)} \qquad P(n) \,.\, n = \sum_{0 < d \leq n} \sum_{i=1}^{q(d,\, n)} P(n - i \,.\, d) I(d) \,.\, d \quad (d, n \in G).$$

Proof. For a fixed $n \in G$, consider the set of all products of irreducibles of M, each of total degree n. By definition, there are $P(n)$ products of this kind. If we multiply them together, we obtain an element m of degree $P(n) \,.\, n$. We shall describe a different way of getting m, which will lead to the expression on the right-hand side of (RF). A similar method has been used by L. Carlitz [2, 3].

We need various subsets of M. Let d be a degree, $0 < d \leq n$. Suppose there are $k = I(d)$ irreducible elements $s_1, s_2, \ldots, s_k$ of degree d in M. Let us write S_i for the set of all products of i (not necessarily distinct) elements out of the set $\{s_1, s_2, \ldots, s_k\}$. S_0 will be taken as a singleton.

For a given natural number $i \leq q(d, n)$, let T_i be the set of all products of irreducibles, each of total degree $n - i \,.\, d$. By definition, $|T_i|$ (the number of elements of T_i), is equal to $P(n - i \,.\, d)$; T_0 is the set considered at the beginning of this proof. U_i shall denote the subset of T_i consisting of all members of T_i that do not contain any of the elements $s_1, s_2, \ldots, s_k$ as factors.

Using the notation $U_i S_j = \{uv\colon u \in U_i,\ v \in S_j\}$, it is obvious that $|U_i S_j| = |U_i|\,|S_j|$. We assert that

$$T_i = \bigcup U_{i+j} S_j,$$

where the union is to be taken over all j from 0 to $q(d, n) - i$. Suppose $u \in U_{i+j}$, $v \in S_j$. We have

$$\deg uv = \deg u + \deg v = n - (i + j) \,.\, d + j \,.\, d,$$

which implies $\deg uv = n - i \,.\, d$, as is easily seen. Hence $uv \in T_i$. On the other hand, let $w \in T_i$. Assume that w contains exactly p factors out of the set $\{s_1, s_2, \ldots, s_k\}$. Then $\deg w = n - i \,.\, d = p \,.\, d + d'$, where d' is the total degree of the remaining factors of w. Clearly,

$$d' + (i + p) \,.\, d = n,$$

hence $i + p \leq q(d, n)$ and $d' = n - (i + p) \,.\, d$. This implies

$$w \in U_{i+p} S_p \quad \text{with } p \leq q(d, n) - i,$$

which proves our claim.

By construction, all sets U and S are pairwise distinct. (Note that we do not consider simply elements of M, but representations by products of irreducibles.) Hence

$$(*) \qquad |T_i| = P(n - i \,.\, d) = \sum_{j=0}^{q(d,n)-i} |U_{i+j}|\,|S_j|.$$

As a special case, consider $T_0 = \bigcup U_j S_j\,(0 \le j \le q(d, n))$, as well as the element m, obtained as the product of all members of T_0. We shall concentrate on the factors $s_1, s_2, \ldots, s_k$ occuring in m.

Let s denote the element $s_1 s_2 \cdots s_k$ of degree $k \,.\, d = I(d) \,.\, d$. If we multiply all members of S_j together, the result will be an element of the form s^{t_j}, where t_j is the number of times any of the elements $s_1, s_2, \ldots$, say s_1, occurs as a factor of the members of S_j. An element of S_j containing s_1 can be written as $s_1 u$, with $u \in S_{j-1}$. There are $|S_{j-1}|$ elements of this kind. Reducing in this way step by step, one arrives at

$$(**) \qquad t_j = |S_{j-1}| + |S_{j-2}| + \cdots + |S_0|.$$

Returning to the element m, by reasons of symmetry, each of the factors $s_1, s_2, \ldots, s_k$ will occur the same number of times, hence m will contain a certain power of their product, say s^t. As is easily seen, the product of all members of $U_j S_j$ contains exactly $|U_j|\, t_j$ factors s. Using $(**)$ one gets

$$t = \sum_{j=1}^{q(d,n)} |U_j|\, t_j = \sum_{j=1}^{q(d,n)} |U_j|(|S_{j-1}| + |S_{j-2}| + \cdots + |S_1| + |S_0|).$$

(Note that $j = 0$ corresponds to $U_0 S_0$, which does not contain any factor s). Rearranging terms on the right-hand side and using $(*)$ gives

$$t = \sum_{i=1}^{q(d,n)} P(n - i \,.\, d).$$

This result is true for fixed d with $0 < d \le n$. The element m itself is a product of elements of the kind s^t, one for each degree d. Hence $\deg m = P(n) \,.\, n$ is equal to

$$\sum_{0<d\le n} \sum_{i=1}^{q(d,n)} P(n - i \,.\, d) I(d) \,.\, d,$$

as was to be shown.

For later use, formula (RF) will be changed somewhat. Consider a fixed degree k, $0 < k \le n$. On the right-hand side of (RF) collect all terms with factor $P(n - k)$. The resulting term is $P(n - k) \sum I(d) \,.\, d$, where the summation is to be extended over all d with the properties: there is an i such that $i \,.\, d = k$ and $1 \le i \le q(d, n)$. As $k \le n$, the second condition is a consequence of the first. By definition, $i = q(d, k) = k/d$. Hence

$$(\mathrm{RF}') \qquad P(n) \,.\, n = \sum_{0<k\le n} P(n - k) \,.\, J(k),$$

where

$$\text{(J)} \qquad J(k) = \sum_{d\mid k} I(d) \, . \, d.$$

It is easy to see that (J) is equivalent to $I(n) \, . \, n = \sum_{d\mid n} \mu(n/d) \, . \, J(d)$, where μ is the ordinary Moebius function.

3. Two examples

Formula (RF) connects the two functions P and I; if either of them is known, the other can be computed recursively. We want to show that two well-known recursion formulae are cases in point.

Let M be the multiplicative monoid of polynomials in one variable over $GF(q)$, with leading coefficient 1; take $G = \mathbf{N}_0$ and for deg the usual degree function. $P(n)$ counts the number of polynomials of degree n, hence $P(n) = q^n$. Formula (RF′) becomes

$$q^n n = \sum_{0<k\leq n} J(k) q^{n-k},$$

which implies $J(k) = q^k$. Introducing this into (J), we obtain

$$\sum_{d\mid n} I(d) d = q^n.$$

This formula is due to Gauss and appears in [4] with a proof contributed by Dedekind using generating functions.

For our second example we use $M = \mathbf{N}$ and $G = \mathbf{N}_0$. Set deg $p_n = n$, where p_n is the nth prime, and extend to a degree function on M in the obvious way. We now have $I(d) = 1$ for each d and formulae (RF′) and (J) become

$$P(n) n = \sum_{0<k\leq n} J(k) P(n-k); \quad J(k) = \sum_{d\mid k} d.$$

As is easily seen, $P(n)$ is the ordinary partition function $p(n)$, whereas $J(k) = \sigma(k)$ in traditional notation. Hence

$$p(n) n = \sum_{0<k\leq n} \sigma(k) p(n-k),$$

a formula first derived by Th. Vahlen [7].

There is an immediate generalization of Vahlen's result. Suppose

$$F = \{f_1, f_2, \ldots\}$$

is a sequence of natural numbers with $f_1 < f_2 < \cdots$. Using the same monoids M and G, but letting deg $p_n = f_n$ for all n, we get $I(d) = 1$ for $d \in F$, $I(d) = 0$ otherwise. Writing $\sigma_F(k) = \sum d$, summed over all divisors of k belonging to F, and $p_F(n)$ for the corresponding partition function (summands of n taken from F only), (RF′) becomes

$$p_F(n) n = \sum_{0<k\leq n} \sigma_F(k) p_F(n-k).$$

This is a recursion formula derived, by means of generating functions, by H. H. Ostmann [6]. He also adds the requirement that the summands of a partition carry a finite number of "colours" each. Of course, the resulting formula is identical to (RF′).

4. Extensions of the examples

L. Carlitz [2] considered polynomials in several variables over $GF(q)$. Using total degree, i.e. sums of exponents of the variables, he obtained the recursion formula

$$P_t(n)n = \sum_{0<k\leq n} J_t(k)P_t(n-k); \quad J_t(k) = \sum_{d\mid k} I_t(d)\, d,$$

where P_t, I_t denote the number of (classes of associated) polynomials and irreducible polynomials, respectively. Of course, Carlitz' formulae are equal to our (RF′) and (J). Since

$$P_t(n) = \left(q^{\binom{n+t}{t}} - q^{\binom{n+t-1}{t}}\right)/(q-1),$$

we have a recursion formula for J_t and hence for I_t.

In a second paper on the subject, L. Carlitz [3] used a different kind of degree, which we shall call a multigrade: for $t = 2$ it is a pair (m, n), where m is the degree in one, n in the other variable. To apply our recursion formula, use the direct sum $\mathbf{N}_0 + \mathbf{N}_0$ as the grading monoid G. With obvious notation, (RF′) will be

$$P(m, n) \,.\, (m, n) = \sum_{(0,0)<(r,s)\leq(m,n)} \sum_i P((m, n) - i \,.\, (r, s))I(r, s) \,.\, (r, s).$$

Splitting into components and writing $ir = x$, $is = y$, one obtains

$$P(m, n)m = \sum_{x=1}^{m} \sum_{y=1}^{n} P(m-x, n-y)x \sum_{i\mid GCD(x,y)} \frac{1}{i} I\left(\frac{x}{i}, \frac{y}{i}\right),$$

the formula derived by Carlitz. (The second component yields an equivalent equation).

We shall now apply the method of multigrades to the partition problem. Using $M = \mathbf{N}$ and $G = \mathbf{N}_0 + \mathbf{N}_0$, let us first assign $(1, i)$ to the ith prime p_i. Then $I(i, j) = 1$ if and only if $i = 1$, $I(i, j) = 0$ otherwise. (RF) becomes

$$P(m, n) \,.\, (m, n) = \sum_{0<s\leq n} \sum_{i=1}^{q} P(m-i, n-is) \,.\, (1, s),$$

where

$$q = \min\left\{m, \left[\frac{n}{s}\right]\right\}.$$

Splitting into components leads to two equivalent formulae, viz.

$$P(m, n)m = \sum_{0<s\leq n} \sum_i P(m-i, n-i).$$

(Note that $P(0, 0) = 1$, but $P(u, 0) = P(0, v) = 0$ for $u \neq 0 \neq v$). Formula (RF′) gives rise to the slightly neater version

$$P(m, n)m = \sum_{0<x\leq n} \sum_{x \mid y} P(m - x, n - y).$$

Keep m fixed and let $n \geq m$. Then $P(m, n)$ counts the number of ways n can be written as a sum of exactly m natural numbers.

There is a much simpler recursion formula for $P(m, n)$, apparently due to Euler: $P(m, n) = P(m - 1, n - 1) + P(m, n - m)$. Its very elementary proof uses the fact that the natural numbers form an arithmetic sequence. Let

$$F = \{f_1, f_2, \ldots\} \quad \text{with } f_1 < f_2 < \cdots$$

and set $\deg p_i = (1, f_i)$. Then the formula

$$P_F(m, n)m = \sum_{\substack{0<s\leq n \\ s \in F}} \sum_{i} P_F(m - i, n - is)$$

again produces the corresponding partition function, while it is doubtful whether a recursion formula of the simpler kind can be derived in case F is not an arithmetic sequence.

By choosing, instead of one subset F as described above, two subsets

$$F = \{f_1, f_2, \ldots\} \quad \text{and} \quad G = \{g_1, g_2, \ldots\}$$

and assigning degree (f_i, g_i) to the prime p_i, formula (RF) leads to

$$P(m, n)m = \sum_{*} \sum_{i} P(m - ir, n - is)r,$$

where the sum $\sum_*$ extends over all pairs $(r, s) \leq (m, n)$ and belonging to the set of all (f_i, g_i). $P(m, n)$ counts the number of solutions of the simultaneous equations

$$m = f_1 x_1 + f_2 x_2 + \cdots$$
$$n = g_1 x_1 + g_2 x_2 + \cdots,$$

a well-known problem in the theory of partition. A generalization to any number of equations is immediate.

5. Norms

In this section, we suppose a norm function has been defined on the monoid M, i.e., a function Nm on M into the positive reals such that $\mathrm{Nm}\, ab = \mathrm{Nm}\, a \,.\, \mathrm{Nm}\, b$. Suppose also that there are only finitely many elements in M of given norm and that $\mathrm{Nm}\, a = 1$ if and only if $a = 1$. log Nm will be a degree function and if its range satisfies the requirements of a grading monoid G, formula (RF) may again be set up. In this section we shall present two examples of this possibility.

Choose $M = \mathbf{N}$ and define Nm $p_n = n + 1$, extending the norm function to M in the obvious way. An easy argument shows, that the number of elements of M of norm n is equal to the number of solutions of the equation

$$n = 2^{x_1}3^{x_2}4^{x_3}5^{x_4}\cdots. \tag{1}$$

The range of log Nm is the set $\{\log n\colon n \in \mathbf{N}\}$ and satisfies the requirements of a grading monoid G. Formula (RF) becomes

$$P(\log n)\,.\,\log n = \sum_{0<\log d\leq \log n}\ \sum_{i=1}^{q(d,\,n)} P(\log n - i\,.\,\log d)I(\log d)\,.\,\log d.$$

The order relation on G is not the one inherited from the reals. We have $\log m \leq \log n$ if and only if $\log m + \log x = \log n$ is solvable, i.e., if and only if $m \mid n$. $q(d, n)$ is the highest value of i such that $i\,.\,\log d \leq \log n$, i.e. such that $d^i \mid n$. Writing, for the moment, $A'(n)$ for $P(\log n)$ and using the fact that $I(\log d) = 1$ for all $d \neq 1$, the formula above can be written in the following way:

$$A'(n)\log n = \sum_{\substack{d\mid n\\ d\neq 1}}\ \sum_{i=1}^{q(d,\,n)} A'(n/d^i)\log d.$$

We shall show that A' may be interpreted as a partition function. For a given n, equation (1) can be reduced to

$$n = d_1^{y(d_1)}\,d_2^{y(d_2)}\cdots d_k^{y(d_k)}, \tag{2}$$

where $d_1, d_2, \ldots, d_k$ denote all divisors of n different from 1. Let $n = q_1^{r_1}q_2^{r_2}\cdots q_t^{r_t}$ be the prime factorization of n. Equation (2) can be written as

$$q_1^{r_1}q_2^{r_2}\cdots q_t^{r_t} = \prod\,(q_1^{s_1}q_2^{s_2}\cdots q_t^{s_t})^{y(s_1,\,s_2,\,\ldots,\,s_t)}, \tag{3}$$

where the product is to be extended over all $(s_1, s_2, \ldots, s_t) \neq (0, 0, \ldots, 0)$ with $0 \leq s_i \leq r_i$. Obviously, this leads to t linear equations in the unknowns y and shows, moreover, that A' does not really depend on n, but rather on the number t of its prime factors and the exponents $r_1, r_2, \ldots, r_t$. We shall write, slightly abusing our notation,

$$A(r_1, r_2, \ldots, r_t)$$

for this function.

We recall some notions of the theory of multisets (see [1], for example). A multiset is an (ordinary) set S and a function $F\colon S \to \mathbf{N}_0$. (Here, $\mathbf{N}_0$ is to be taken with its ring structure). A function $G\colon S \to \mathbf{N}_0$ is called a submultiset of (S, F), denoted by $G \subseteq F$, if $Gs \leq Fs$ for all $s \in S$. In the sequel, we shall always omit the null multiset: $Os = 0$ for all $s \in S$. A partition of a multiset (S, F) is a function P on the set of all submultisets of F into $\mathbf{N}_0$ with the property $\sum_{G\subseteq F}(PG)(Gs) = Fs$ for all $s \in S$.

Assume S finite with t elements; we may require $Fs \neq 0$ for all s. F can be characterized by a sequence $(r_1, r_2, \ldots, r_t)$ of natural numbers, a submultiset G by $(s_1(G), s_2(G), \ldots, s_t(G))$ with $0 \leq s_i(G) \leq r_i$, not all $s_i(G) = 0$. A partition P of (S, F) consists of numbers $PG = y_G$ for each G with the condition $\sum_{G \subseteq F} y_G s_i(G) = r_i$ for $i = 1, 2, \ldots, t$.

It is now obvious how the problem of partitions of finite multisets is related to equation (3). Any solution $y(s_1, s_2, \ldots, s_t)$ of (3) corresponds to a partition P with

$$PG = y(s_1, s_2, \ldots, s_t)$$

and vice versa. Hence $A(r_1, r_2, \ldots, r_t)$ counts the number of partitions of the corresponding multiset. The recursion formula for A' can be rewritten as

$$\text{(4)} \qquad A(r_1, r_2, \ldots, r_t) \log q_1^{r_1} q_2^{r_2} \cdots q_t^{r_t} = \sum_{(s_1, s_2, \ldots, s_t)} \sum_i A(r_1 - is_1, \ldots, r_t - is_t) \log q_1^{s_1} \cdots q_t^{s_t},$$

with the obvious summations over $(s_1, \ldots, s_t)$ and i.

We consider two limiting cases. Let S consist of only one element s. If $Fs = m$, a partition of (S, F) is the same as a number-theoretic partition of the number m and equation (4) is just Vahlen's recursion formula of Section 3.

Next, let (S, F) be an ordinary set, i.e., $Fs = 1$ for all $s \in S$. A submultiset is a subset of S and a partition is an ordinary partition of S into subsets. (4) becomes

$$A(1, 1, \ldots, 1) \log q_1 \cdots q_t = \sum_{(s_1, \ldots, s_t)} A(1 - s_1, \ldots, 1 - s_t) \log q_1^{s_1} \cdots q_t^{s_t},$$

where $(s_1, s_2, \ldots, s_t)$ runs through all 0-1-sequences of length t except $(0, 0, \ldots, 0)$.

As is easily seen, A depends only on the number of 1's appearing as arguments. Let us write $B(k)$ if there are k of them. On the right-hand side of the equation $B(k)$ will appear whenever there are exactly k zeros in the sequence $(s_1, \ldots, s_t)$. By an easy argument, the factor of $B(k)$ is seen to be $\log (q_1 q_2 \cdots q_t)^u$ with $u = \binom{t-1}{k}$. Taking exponentials we get

$$B(t) = \sum_{k=0}^{t-1} \binom{t-1}{k} B(k); \quad B(0) = 1.$$

$B(t)$ is known as a Bell number and the equation we just derived is the standard recursion formula for Bell numbers. (See [1], for example.)

One gets further results by the method of multigrades. As in Section 4, we take $M = \mathbf{N}$, while for G we choose the direct sum $\mathbf{N}_0 + \log \mathbf{N}$. The order relation on G is now $(a, \log b) \leq (c, \log d)$ if and only if $a \leq c$ and $b \mid d$. Assign degree $(1, \log (i + 1))$ to the ith prime p_i. $P(k, \log n)$, the number of elements of degree $(k, \log n)$, is equal to the number of solutions of the equation

$$(k, \log n) = (1, \log 2)x_1 + (1, \log 3)x_2 + \cdots + (1, \log n)x_{n-1},$$

which is equivalent to the pair of equations

$$n = 2^{x_1} 3^{x_2} \cdots n^{x_{n-1}}, \quad x_1 + x_2 + \cdots + x_{n-1} = k.$$

A solution of these equations can be interpreted as a partition of a multiset with the number of submultiset making up the partition fixed to k. If

$$n = q_1^{r_1} q_2^{r_2} \cdots q_t^{r_t}$$

is the prime factorization of n and if we write $A(k, r_1, \ldots, r_t)$ for $P(k, \log n)$, then formula (RF) leads, by arguments used before, to the following equations:

$$A(k, r_1, \ldots, r_t)k = \sum_{(s_1, \ldots, s_t)} \sum_i A(k - i, r_1 - is_1, \ldots, r_t - is_t),$$

$$A(k, r_1, \ldots, r_t) \log q_1^{r_1} \cdots q_t^{r_t}$$
$$= \sum_{(s_1, \ldots, s_t)} \sum_i A(k - i, r_1 - is_1, \ldots, r_t - is_t) \log q_1^{s_1} \cdots q_t^{s_t}.$$

We consider once more two limiting cases. If the underlying set of the multiset considered has just one element s and if $Fs = m$, $A(k, m)$ will be the number of partitions of m into k summands and our equations are identical to the corresponding equations of Section 4. If the multiset is an ordinary set with m elements, our equations above reduce to

$$A(k, 1, 1, \ldots, 1)k = \sum_{(s_1, \ldots, s_t)} A(k - 1, 1 - s_1, \ldots, 1 - s_t),$$

$$A(k, 1, 1, \ldots, 1) \log q_1 \cdots q_t = \sum_{(s_1, \ldots, s_t)} A(k - 1, 1 - s_1, \ldots, 1 - s_t) \log q_1^{s_1} \cdots q_t^{s_t},$$

$(s_1, s_2, \ldots, s_t)$ running through all 0-1-sequences of length t except $(0, 0, \ldots, 0)$. Again, A depends only on the number of 1's appearing after the first argument; let us write $S(r, k)$ for an A with r ones. We get

$$S(t, k)k = \sum_{r=0}^{t-1} \binom{t}{r} S(r, k - 1) \tag{5}$$

$$S(t, k) = \sum_{r=0}^{t-1} \binom{t-1}{r} S(r, k - 1). \tag{6}$$

The number of partitions, $S(t, k)$, of a t-element set into k subsets, is a Stirling number of the second kind. (5) and (6) are standard recursion formulae for them. (Given (6), (5) is equivalent to

$$S(t, k) = S(t - 1, k)k + S(t - 1, k - 1)).$$

6 Algebraic number fields

Let A denote the ring of algebraic integers of an algebraic number field; for $a \in A$, let $\mathrm{Nm}\, a$ be the norm of the principal ideal Aa. As is well known, the number of ideals of given norm is finite. Since every element of A may be written as a product of irreducibles—not necessarily in a unique way—and as log Nm is again a degree function, we have new cases of the situation (M, G, deg) to which (RF) is applicable. However, it is far from trivial to evaluate the function I and we shall only present examples of quadratic number fields, with class numbers 1 and 2.

Suppose A is the ring of algebraic integers of $\mathbf{Q}(\sqrt{d})$ of class number 1. A has unique representation by irreducibles and it suffices to represent rational primes. One has to distinguish between ramified, inert and decomposed primes, however.

As a first example, consider $A = \mathbf{Z}[\sqrt{-1}]$. The number 2 is the only ramified prime with $2 = (1 + i)(1 - i)$ and $\mathrm{Nm}\,(1 + i) = 2$. We have p inert if and only if $p \equiv 3 \bmod 4$ and $\mathrm{Nm}\, p = p^2$. Also, q is decomposed if and only if $q \equiv 1 \bmod 4$; we have

$$q = (a + bi)(a - bi) \quad \text{with } \mathrm{Nm}\,(a + bi) = a^2 + b^2 = q.$$

These facts allow one to evaluate the function I: $\mathrm{I}(2) = 1$; $I(p^2) = 1$ for $p \equiv 3 \bmod 4$; $I(q) = 2$ for $q \equiv 1 \bmod 4$; $I(k) = 0$ otherwise. (RF) becomes (the notation being obvious, empty sums counting as 0):

$$\text{(7)} \quad P(n) \log n$$
$$= \sum_i P(n/2^i) \log 2 + \sum_{p^2 | n} \sum_i P(n/p^{2i}) \log p^2 + \sum_{q | n} \sum_i P(n/q^i) \,.\, 2 \log q.$$

To solve this recursion, suppose $n = 2^u \prod_r p_r^{2v_r} \prod_s q_s^{w_s}$ is the prime decomposition of n, symbols p_r and q_s denoting inert and decomposed primes, respectively. We may use even exponents for primes p_r, for if such a prime occurs with odd exponent, $P(n) = 0$. Taking exponentials on both sides of equation (7) and comparing exponents of like prime powers leads to

$$uP(n) = \sum_i P(n/2^i); \quad v_r P(n) = \sum_i P(n/p_r^{2i}); \quad w_s P(n) = 2 \sum_i P(n/q_s^i).$$

If from the first of these equations one subtracts the corresponding one for $n/2$, one arrives at $uP(n) = uP(n/2)$, which shows that $P(n)$ is independent of the prime factor 2. The same result follows from the second group of equations for the prime factors p_r. Finally, subtraction of

$$(w_s - 1)P(n/q_s) = 2 \sum_i P(n/q_s^{i+1})$$

from the third group of equations leads to

$$P(n) = \frac{w_s + 1}{w_s} P(n/q_s) = \frac{w_s + 1}{w_s} \frac{w_s}{w_s - 1} P(n/q_s^2) = \cdots.$$

Hence $P(n) = (w_s + 1)P(n/q_s^{w_s})$. This essentially solves the recursion and we arrive at the following result: If n decomposes into prime powers as given above, then $P(n)$ is equal to 1 for $n = 1$, to 0 if at least one of the exponents v_r is odd, to $\prod_s (w_s + 1)$ if $n \neq 1$ and all v_r are even.

Each element $a + bi$ of norm n is connected to a solution of the Diophantine equation $n = a^2 + b^2$. One usually considers numbers associated to $a + bi$ or $a - bi$ as different solutions, hence $r(n)$, the number of solutions of $n = x^2 + y^2$, is equal to $4P(n)$. The resulting formula

$$r(n) = 4 \prod_s (w_s + 1)$$

is due to Jacobi and Gauss. (For example, see [5].)

The derivation of (7) does not depend on the specific value -1 for d, but works the same way for any quadratic number field of class number 1. The only thing to take care of are ramified primes r, which can either be reducible in the ring of algebraic integers and lead to $I(r) = 1$, or else simulate inert primes by having $I(r^2) = 1$. In any case, if $P_d(n)$ denotes the number of algebraic integers of norm n in $\mathbf{Q}(\sqrt{d})$ (of class number 1), then essentially

$$P_d(n) = \prod_s (w_s + 1),$$

where w_s is the exponent of a decomposed prime dividing n, primes with the Legendre symbol

$$\left(\frac{d}{q_s}\right) = 1.$$

To interpret $P_d(n)$ as the number of representations of n by a corresponding binary form one has to take the necessary precautions as to positive d (and infinitely many units), to $d \equiv 1 \bmod 4$ and to the special case $d = -3$.

As a final example, we shall evaluate $P(n)$ for the field $\mathbf{Q}(\sqrt{-5})$, which is of class number 2. We shall use variables p, q, r for rational primes congruent mod 20 to 11, 13, 17, 19, to 1,9 and to 3,7, respectively. The function I can be described as follows: $I(p^2) = 1$, $I(q) = 2$, $I(r^2) = 3$, $I(2r) = 2$, $I(r_1 r_2) = 4$ $(r_1 \neq r_2)$, $I(4) = I(5) = 1$, $I(n) = 0$ otherwise. For a proof of these equations, see [8], for example. Formula (RF) has the following form:

$$\begin{aligned} P(n) \log n = {} & \sum_{p^2 | n} \sum_i P(n/p^{2i}) \log p^2 + \sum_{q | n} \sum_i P(n/q^i) \,.\, 2 \log q \\ & + \sum_{r^2 | n} \sum_i P(n/r^{2i}) \,.\, 3 \log r^2 + \sum_{2r | n} \sum_i P(n/(2r)^i) \,.\, 2 \log (2r) \\ & + \sum_{r_u r_v | n} \sum_i P(n/(r_u r_v)^i) \,.\, 4 \log (r_u r_v) + \sum_i P(n/4^i) \log 4 \\ & + \sum_i P(n/5^i) \log 5. \end{aligned}$$

One can, as before, split up this equation with respect to the prime divisors of n and then try to find an explicit value of $P(n)$ as a function of the exponents of these divisors. It turns out that $P(n)$ is independent of the exponents of p (they must, however, be even) and of 5, depends on those of q as in the Gauss-Jacobi theorem, but the dependence on the exponents of 2 and r is much more intricate and requires further study. For example,

$$P(r^a) = (a+2)(a+4)/8 \quad \text{for even } a,$$

while

$$P(32r^a) = (3a^2 - 4a + 5)/2 \quad \text{for odd } a.$$

Another inherent disadvantage is the fact that $P(n)$ is not equal to the number of elements of norm n, but to the number of different products of irreducibles, each of total norm n. For instance, $P(216) = 10$, corresponding to the products

$$2 \cdot 3 \cdot (1+\sqrt{-5}), \quad (1+\sqrt{-5})^2(1-\sqrt{-5}), \quad (1+\sqrt{-5})^3,$$
$$2 \cdot (1+\sqrt{-5})(2-\sqrt{-5}), \quad 2 \cdot (1-\sqrt{-5})(2-\sqrt{-5})$$

and their conjugates, while there are only four elements of norm 216.

References

1. M. Aigner, *Kombinatorik I: Grundlagen und Zähltheorie*, Springer Verlag, New York, 1975.
2. L. Carlitz, *The distribution of irreducible polynomials in several indeterminates*, Illinois J. Math., vol. 7 (1963), pp. 371–375.
3. ———, *The distribution of irreducible polynomials in several variables II*, Canadian J. Math., vol. 17 (1965), pp. 261–266.
4. C. F. Gauss. *Werke 2*, Nr. 342–347, Göttingen, 1876.
5. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, third edition, Oxford Univ. Press, London, 1954.
6. H. H. Ostmann, *Ueber eine Rekursionsformel in der Theorie der Partitionen*, Math. Nachr., vol. 13 (1955), pp. 157–160.
7. Th. Vahlen, *Beiträge zu einer additiven Zahlentheorie*, J. reine angew. Math. vol. 112 (1893), pp. 1–36.
8. P. Wilker, *Die irreduziblen Zahlen des Bereichs* $Z[\sqrt{-5}]$, Elem. Math., vol. 34 (1979), pp. 75–82.

Universität Bern
Bern, Switzerland